Incident Response Policy

Incident Response Policy • Version 1 • 8 October 2026

Department:	Information Security
Document Owner:	Security Officer
Owner Title:	Security Officer
Classification:	Confidential
Effective Date:	8 October 2026
Review Cycle:	Annually

1. Purpose, scope and definitions

This policy establishes how 786 Cyber detects, responds to and recovers from security inc
protect our systems, data and operations.

Definitions

A **security event** is any observable occurrence in our systems or networks, such as a u
file access or network connection. Not all events are significant.

A **security incident** is an event that compromises or threatens the confidentiality, integri
availability of our information assets. Examples include:

- Unauthorised access to systems or data
- Malware infections or ransomware attacks
- Data theft or exfiltration
- Denial of service attacks
- Loss or theft of devices containing business data
- Phishing attacks resulting in credential compromise
- Misuse of access privileges by staff or third parties

A **personal data breach** is an incident that affects personal data we process, including
or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal
includes breaches affecting employee, customer or supplier information.

Scope

This policy applies to:

- All information systems, networks and infrastructure operated or managed by 786 Cyber
- Data we hold, process or transmit, including client data, business information and person
- All employees, contractors, consultants and third parties with access to our systems or d
- Physical security breaches affecting our premises and equipment

The procedures defined in this policy must be followed by all personnel. Managers are res
ensuring their teams understand and comply with incident response requirements.

2. Roles and the incident response team

The **Information Security Lead** serves as the incident lead, with overall responsibility fo coordinating the incident response process. The incident lead is supported by designated who can assume this role when the lead is unavailable.

The incident response team comprises members from relevant business functions, includi operations, management, and communications. Team members are identified based on th expertise and ability to support incident handling activities.

We maintain an up-to-date contact list for all incident response team members, including p alternative contact methods. This list is reviewed quarterly and updated whenever personn occur. Contact details are stored securely and remain accessible to authorised personnel

External contacts

We maintain relationships with key external parties who may need to be engaged during a

- **IT provider** – for technical support and infrastructure management
- **Insurer** – to notify of potential claims and obtain guidance on incident handling
- **Legal advisers** – for advice on contractual, regulatory, and liability matters
- **Regulators** – including the Information Commissioner's Office for data breach notifica relevant sector regulators
- **Law enforcement** – such as Action Fraud or local police for criminal matters

Contact details for these external parties are documented alongside internal team contact reviewed regularly to ensure accuracy. We establish the circumstances under which each contact must be engaged, including timeframes for regulatory notifications. The incident le responsible for determining when external parties should be contacted and for managing t communications.

3. Reporting and triage

All personnel, contractors, and third parties must report any suspected information securit immediately upon discovery. Reports should be submitted through the IT Service Desk tic system or, if unavailable, by emailing security@786cyber.co.uk or telephoning the IT Servi Outside normal business hours, incidents must be reported using the emergency contact provided in the staff handbook.

Upon receipt of a report, the Incident Response Team will conduct an initial assessment to the incident's nature, scope, and potential impact. This assessment evaluates factors inclu

- Extent of data compromise or system disruption
- Number of users or systems affected
- Business criticality of impacted services
- Potential regulatory or legal implications
- Reputational risk to 786 Cyber or clients

Based on this assessment, incidents are assigned one of four severity levels:

- **Critical**: Significant data breach, complete service outage, or threat to business contin
- **High**: Major system compromise, potential data loss, or serious service degradation
- **Medium**: Limited system impact, contained security breach, or moderate service disru
- **Low**: Minor security concern, isolated incident, or minimal business impact

The Incident Response Manager has final authority on severity classification and may adju
as new information emerges.

All incidents are logged in the central Incident Register from the moment of first report, reg
severity. The log captures the date and time reported, initial description, reporter details, a
severity, and response actions taken. This register provides an audit trail and enables trend
to improve our security posture.

4. Containment, eradication and recovery

Upon confirmation of a security incident, containment actions must be taken promptly to li
impact and prevent further damage. Containment measures include:

- Isolating affected devices from the network
- Disabling compromised user accounts or credentials
- Blocking malicious IP addresses or domains at the perimeter
- Restricting access to affected systems or data

The IT Security Manager or IT Director must authorise all containment actions. In their abs
Incident Response Team Lead may authorise urgent containment measures, with retrospe
approval documented within 24 hours.

Evidence preservation

We must preserve all evidence relating to the incident to support investigation, potential le
proceedings and lessons learnt activities. The following must be collected and secured:

- System and application logs from affected and related systems
- Forensic images of affected devices before remediation
- Network traffic captures where available
- Screenshots and photographs documenting the incident state
- A detailed timeline recording all actions taken, decisions made and personnel involved

Evidence must be stored securely with controlled access and documented chain of custod
maintained throughout.

Recovery procedures

Recovery activities commence only after the incident has been fully contained and eradica
Systems must be restored from known-good backups that predate the incident or compron
Before returning systems to service, we must:

- Verify backups are free from malware or compromise
- Apply all current security patches and updates
- Change all relevant passwords and credentials
- Conduct functionality and security testing
- Monitor systems closely for signs of recurring issues

The IT Security Manager must approve all systems before they return to production use.

5. Personal data breaches and regulatory notification

Every incident is assessed to determine whether it involves personal data. This assessme
part of the initial incident triage and is documented in the incident record.

When an incident meets the threshold for a reportable personal data breach, we notify the Information Commissioner's Office within 72 hours of becoming aware of the breach. The Information Security Officer or designated deputy is responsible for determining whether a reportable and for submitting the notification. Where the full details are not yet known withi deadline, we submit an initial notification with available information and provide updates as investigation progresses.

If a personal data breach is likely to result in a high risk to the rights and freedoms of indiv notify affected individuals without undue delay. The notification includes clear information a nature of the breach, likely consequences, and measures individuals can take to protect th The data protection lead determines when individual notification is required and approves and method of communication.

786 Cyber falls within scope of NIS regulations. When an incident affects network and info systems and meets the significance threshold, we adhere to the following notification time

- Early warning to the relevant authority within 24 hours of becoming aware
- Full notification submitted within 72 hours
- Final incident report provided within one month

The Incident Manager coordinates all regulatory notifications and maintains records of wh reported, when, and to which authorities. These records form part of the overall incident documentation and are retained according to our data retention schedule.

6. Communication

During an incident, controlled communication is essential to protect our reputation, mainta customer confidence, and prevent premature disclosure of vulnerabilities.

Authorised Spokespersons

Only the following individuals may communicate about security incidents to external partie

- The Chief Information Security Officer may speak to customers, media, and regulatory b
- The Managing Director may speak to customers and media
- The Incident Response Manager may speak to customers when authorised by the CISO

No other staff members may discuss incidents with external parties without explicit written authorisation from the CISO or Managing Director.

Internal Communication

During incident response:

- The Incident Response Manager will brief relevant staff on a need-to-know basis
- All internal communications about the incident must use encrypted channels
- Staff must not discuss the incident in public areas, on personal devices, or with colleague involved in the response
- Team members must refer any external enquiries to the authorised spokespersons imme

Confidentiality Requirements

All personnel involved in incident response must maintain strict confidentiality until the inci resolved and official communication is approved. This includes:

- Not discussing the incident on social media or public forums
- Not sharing technical details outside the response team
- Not speculating about causes, impacts, or responsible parties
- Protecting any customer data or sensitive information discovered during investigation

We will communicate with affected customers and regulatory authorities according to our l
obligations and the Communications Plan developed during the incident response process
statements will only be issued after thorough review by senior management and legal cou
appropriate.

7. Lessons learned and testing

Following every incident, we conduct a post-incident review within two weeks of resolution
Incident Response Manager chairs this review meeting, bringing together all personnel inv
the response.

The review must identify:

- What occurred and the root cause of the incident
- What worked well during the response
- What could be improved in our processes, tools or communications
- Specific actions required to prevent recurrence or improve response capability

Each action identified must be assigned to a named individual with a realistic completion d
Incident Response Manager tracks these actions through to completion and reports progr
Information Security Manager monthly.

We document all findings and actions in a post-incident review report, which is stored secu
made available to relevant stakeholders. Trends and recurring issues identified across mul
incidents inform updates to this policy and our wider security programme.

Testing Programme

We test this incident response plan every 12 months through a structured exercise. The In
Security Manager arranges these tests and ensures appropriate scenarios are selected to
our procedures and capabilities.

Tests may take the form of tabletop exercises, simulations or technical drills, depending on
specific aspects of the plan requiring validation. We include relevant personnel from IT, ma
and other business functions as appropriate to the scenario.

Following each test, we review performance and identify any gaps or weaknesses. We upd
plan within one month of the test to address findings and incorporate lessons learned. Cha
communicated to all relevant personnel and reflected in subsequent training activities.

8. Ownership, review and exceptions

The Information Security Lead owns this policy and is responsible for maintaining its curre
effectiveness. The policy must be approved by senior management prior to implementation
following any material revisions.

This policy is reviewed every 12 months to ensure it remains appropriate and aligned with
objectives and the threat landscape. Reviews are also conducted following significant secu
incidents, major organisational changes, or updates to our operational environment that m

incident response capabilities.

Exceptions to this policy may be necessary in specific circumstances. Any request for an e
must:

- Be submitted in writing to the Information Security Lead with clear justification
- Include details of compensating controls or alternative measures
- Be approved by senior management before implementation
- Identify a named risk owner who accepts accountability for the exception
- Be recorded in the exception register maintained by the Information Security Lead
- Include an expiry date, after which the exception lapses unless formally renewed

All exceptions are reviewed as part of the annual policy review cycle and may be revoked
circumstances change or risks become unacceptable.

Failure to comply with this policy may result in disciplinary action in accordance with 786 C
normal disciplinary procedures. The severity of the breach and any mitigating circumstanc
considered when determining appropriate consequences. Serious or repeated violations m
in formal disciplinary measures up to and including termination of employment. Breaches
contractors or third parties may result in termination of contracts or access rights.